DWIGHT C. HOLTON, OSB #090540
United States Attorney
District of Oregon
GREGORY R. NYHUS, OSB # 913841
Assistant United States Attorney
1000 S.W. Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
greg.r.nyhus@usdoj.gov
Attorneys for United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA	**09-CR-321-KI**
v.	**GOVERNMENT'S BRIEF REGARDING DEFENDANTS' MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP AND EXTERNAL HARD DRIVE**
HOCK CHEE KOO, THONGSOUK SOUTAVONG, et al.,	
Defendants.	

The United States of America, by Dwight C. Holton, United States Attorney for the District of Oregon, through Gregory R. Nyhus, Assistant United States Attorney (AUSA) for the District of Oregon, provides this closing brief regarding defendants' motion to exclude from evidence forensic images taken from the Wu laptop and external hard drive.

Defendants seek to exclude a forensic image taken by the FBI of defendant Wu's laptop computer and a copy of the same (the Acronis image) because they claim the original Wu laptop hard drive lacked evidentiary integrity when images were created from it. In sum, the defendants assert that the images taken of the Wu laptop cannot be properly authenticated.

The government maintains that the evidence is admissible, that it can be properly authenticated and that arguments regarding the quality of the evidence and the nature of its

acquisition address its probative value. Evidence being challenged on authenticity grounds should be admitted so long as a reasonable juror could find that evidence to be authentic. Therefore, defendants' arguments are more appropriately directed to the weight the jury should give the evidence, not to the authenticity and/or admissibility of that evidence.

FACTUAL BACKGROUND

Lawrence "Drew" Hoffman is the principal in The Hoffman Group ("THG"), a company that manufactures products for the after-market automobile industry. The majority of THG's manufacturing occurs in China., and THG maintains a China office that oversees this manufacturing.

Defendants in this case are former employees of THG . Wu's role was to coordinate the manufacturing of products in China, while defendants Khoo and Soutavong filled other duties locally. Wu's employment with THG was regulated by several agreements, one of which was a non-disclosure agreement.

THG maintained much of its proprietary information regarding product development, processes and factory details in a database that Hoffman believed to be secure.

In August 2006, Hoffman discovered on eBay an auction selling a product that appeared to be identical to one of THG's products. Hoffman researched the eBay sale and determined that the product was being sold by THG's former employees Soutavong, Khoo, and Wu. Hoffman eventually hired a private investigator who purchased said product on the eBay site.

On September 12, 2006, Hoffman contacted the FBI and spoke with Special Agent (SA) Phil Slinkard, who took the initial report and opened an investigation.

At Hoffman's request, on October 17, 2006, Wu flew to the United States. Hoffman obtained the THG laptop assigned to Wu and gave it to Mark Hansen, a forensics expert and computer analyst. After Wu turned over the laptop, Hansen used Acronis software to copy an image of the hard drive onto an external USB hard drive.

Hoffman then took the laptop home, turned it on and examined some of its contents. He attempted to copy the contents of one folder onto a thumb drive, but was unable to do so. Hoffman noted that a majority of the operating system was in Chinese. He was also unaware of any deletions or changes he may have made to the computer during that time.

Defendants' expert contends that the Wu laptop suffered multiple deletions and showed evidence of suspicious tampering during the time it was in Hoffman's possession. According to his analysis, some 255 files were either altered or deleted, leading to his conclusion that because Hoffman accessed the computer in the manner in which he did, he destroyed the evidentiary integrity of the computer: forensically, it was not the same as it was when initially recovered from Wu. Further, because the Acronis image was not a forensic image and did not copy the contents of the Wu laptop bit by bit, the metadata and other latent material was not copied, rendering it an unreliable source of verification against the Wu laptop. Defendant's expert, however, was unable to state with any certainty whether any of the content revealed in native format[1] was different. In fact, he stated that he did not print or boot up or compare any of the material found on either the Wu laptop, its image or the Acronis copy. The impact of any

[1]A native format, in the context of software applications, refers to the file format which the application works with during creation, edition or publication of a file. A Word Perfect file may open in Word, but the native format is Word Perfect.

alteration at a bit level (or even the deletion or alteration of meta data) on any of the evidence as rendered in a readable format, therefore, is unclear.

On October 20, 2006, Hoffman brought the laptop to the FBI's Northwest Regional Computer Forensic Laboratory, where he met with FBI Special Agent Phil Slinkard. With SA Slinkard present, Hoffman attached an external USB drive to the computer. Hoffman then transferred a copy of a folder on the laptop labeled "Private." SA Slinkard monitored the entire transfer, which took about fifteen minutes. Hoffman also turned over the USB drive containing the image of the laptop obtained by Mark Hansen.

The laptop and the drive were then checked into the Evidence Control Facility on November 1, 2006. Sometime between November 3 and November 6, 2006, forensic images were made of both the Wu Laptop and the Acronis image, after which the original materials were checked back into evidence. According to administrative review of the forensic process, the equipment used by the forensic examiner, FBI Special Agent Joel Brillhart, was properly calibrated and there were no anomalies recorded with respect to dates and times. Administrative review of the forensic examination also revealed that hash values for both images matched hash values for the original values made of the Wu laptop and the Acronis copy, indicating that the forensic process resulted in an exact copy of the original.

At issue, therefore is the admissibility of evidence gleaned from the image of the Wu laptop in the form of chats, emails and other electronic evidence, including the Platipus database and its contents.

///

///

ARGUMENT

Defendants' argument appears to be two-fold: First, defendants allege that, because the Wu laptop was mishandled by Hoffman, and potential evidence was destroyed, the subsequent image of the Wu laptop is merely an image of already tainted evidence. As such, it cannot be reliably authenticated as a forensic image of the laptop under Wu's control. Second, the defendants contend that there were issues regarding the forensic process by which the images were created, causing spoilation of the evidence to such an extent that the image taken of the laptop and the Acronis copy cannot be relied upon.

A. Authentication

The "[r]esolution of whether evidence is authentic calls for a factual determination by the jury and admissibility, therefore, is governed by the procedure set forth in Federal Rule of Evidence 104(b) 'relating to matters of conditional relevance generally.' " Fed .R. Evid. 901(a) advisory committee's notes state that authentication and identification represent a special aspect of relevancy.... This requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b). Determining whether the images are authentic, and therefore relevant, is a two step process. First, before admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic. Then, because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims. *Lorraine v. Markel American Insurance Company*, 241 FRD 534, 539 (2007).

The foundational "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Rule 901(a) only requires the government to make a *prima facie* showing of authenticity or identification "so that a reasonable juror could find in favor of authenticity or identification."

> Although the district court is charged with making this preliminary determination, because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims. Because the ultimate resolution of authenticity is a question for the jury, in rendering its preliminary decision on whether the proponent of evidence has laid a sufficient foundation for admission the district court must necessarily assess the adequacy of the showing made before the jury.

United States v. Branch, 970 F.2d 1368, 1370 (4th Cir.1992).

The proponent of the evidence need only make a prime facie case that the evidence is what it purports to be. The standard of proof is not stringent - quite the opposite: the proponent need only show sufficient facts to allow a finding to be made supporting the conclusion that an item is what it purports to be. *United States v. Dhinsa*, 243 F.3d 635, 658-59 (2nd Cir. 2001) (noting Rule 901 "does not erect a particularly high hurdle," and that hurdle may be cleared by "circumstantial evidence") (quoting *United States v. Ortiz*, 966 F.2d 707, 716 (1st Cir. 1992)).

Any questions about the weight of the evidence, its credibility or whether, in fact, the evidence can be finally authenticated is a matter for the jury. *Orr v. Bank of America*, 285 F.3d 764, 773 n.6 (9th Cir. 2002) ("Once the trial judge determines that there is prima facie evidence of genuineness, the evidence is admitted, and the trier of fact makes its own determination of the evidence's authenticity and weight."); *United States v. Paulino*, 13 F.3d 20, 23 (1st Cir. 1994) ("In respect to matters of authentication, the trial court serves a gatekeeping function. If the

court discerns enough support in the record to warrant a reasonable person in determining that the evidence is what it purports to be, then Rule 901(a) is satisfied and the weight to be given to the evidence is left to the jury");

In fact, arguments regarding spoilation, alteration, forgery and even improper methods by which the items or evidence were collected is reserved properly for the jury as part of its deliberative process to determine what weight, if any, to give to the evidence in question. Once the government meets the threshold burden of providing facts from which a reasonable juror could conclude that the item is what it purports to be, "the credibility or probative force of the evidence offered is, ultimately, an issue for the jury." *United States v. Chu Kong Yin*, 935 F.2d 990, 996 (9th Cir. 1991); *see also, Lexington Ins. Co. v. Western Pennsylvania Hosp.*, 423 F.3d 318, 328-29 (3d Cir. 2005) ("Once a prima facie case is made, the evidence goes to the jury and it is the jury who will ultimately determine the authenticity of the evidence, not the court. The only requirement is that there has been substantial evidence from which they could infer that the document was authentic.").

This relationship is best illustrated in *United States v. Black*, 767 F.2d 1334, 1342 (9th Cir.) a fraud and tax prosecution in which confirmation slips reflecting futures transactions in T-Bill and silver futures made by a commodities dealer were authenticated by the fact that they were found in the defendant's possession. "Whether the confirmation slips were forgeries, whether the defendant obtained the documents in the fashion he described, or whether he was responsible for their fabrication were all issues for the jury to decide." In *United States v. Safavian*, 435 F.Supp.2d, 36 (D.D.C. 2006) the court analyzed the admissibility of e-mail, noting,

> "[t]he question for the court under Rule 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is....' The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so."

435 F.Supp.2d at 38.

Here, there is ample evidence from which a rational trier of fact could determine that the images of both the Wu laptop and the Acronis copy are authentic - they are what they purport to be - even with the allegedly apparent deficiencies in the chain of custody. The allegations of deficiencies in the chain of custody have not been established to be detrimental to the content of the material that would have been displayed in a native format, but rather seem to be arguments that - outside of the government's control - material may have been lost or changed. Assigning any weight to any of those considerations in evaluating the content of the evidence before it is clearly a matter for the jury to decide.

B. Spoilation

Although the standards are different, the issues presented with respect to spoilation are interrelated. Defendants' argument that spoilation of evidence under government control is grounds for suppression because it cannot be authenticated borrows from the legal principles outlined above as well as the following additional points .

"Unless a criminal defendant can show bad faith on the part of the police, a failure to preserve potentially useful evidence does not constitute a denial of due process of the law." *Arizona v. Youngblood* , 488 U.S. 51, 58 (1989). Where forensic examinations are conducted in a "professional and reasonable manner," those examinations are presumed to uphold the integrity of evidence. *Youngblood*, 488 U.S. at 59. The trial court determines "whether

proffered evidence has enough prima facie trustworthiness to warrant its consideration by the jury." *United States v. King*, 472 F.2d 1, 7 (9th Cir. 1973).

Even where questions about evidentiary reliability that flow from a possible break in the chain of custody also inform the weight, not admissibility, of the evidence. *United States v. Vansant*, 423 F.2d 620, 621 (9th Cir.), *cert. denied*, 400 U.S. 835 (1970); *United States v. Godoy*, 528 F.2d 281, 284 (9th Cir.1975). The possibility of misidentification or alteration must be "eliminated, not absolutely, but as a matter of reasonable probability." *United States v. Allen*, 106 F.3d 695, 700 (6th Cir.1997) (quoting *United States v. McFadden*, 458 F.2d 440, 441 (6th Cir.1972) (internal quotation marks omitted)).

Even if the court were to find that there were errors or omissions in the forensic process under consideration (there is no dispute that the forensic images created by the FBI had the same hash values as their original sources, indicating exact copies) the evidence is still admissible and any contentions about errors are for the jury. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988) (Accuracy of computer records and evidentiary reliability proper subject for cross examination and jury deliberation). Even where allegations that evidence is tainted by intentional tampering by the custodians, trustworthiness concerns are appropriately directed to weight and not admissibility. *United States v. Bonallo*, 858 F.2d, 1427, 1436 (9th Cir. 1988) (Merely raising the possibility of tampering, or suggesting that manipulation or alteration of the evidence could have occurred is not sufficient to render evidence inadmissible). When the reliability of evidence presented by an expert is at issue, "[v]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof

are the traditional and appropriate means of attacking shaky but admissible evidence." *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 596 (1993).

In the instant case, the government has authenticated the data in the laptop image and the Acronis image by demonstrating that standard forensic procedures were applied to the acquisition and handling of the evidence. In spite of defendants' arguments to the contrary, an administrative review of the forensic process showed that the images were acquired under conditions that were forensically sound, with equipment that was properly calibrated by qualified personnel and, finally, that the hash values matched. Under these circumstances, the government has clearly established a prime facie showing that the images acquired by forensic personnel were done so under circumstances that *the jury* may find reasonable and compelling. This indicia of trustworthiness is all the government must muster in a showing of authentication. Moreover, what is being offered by the government, the image of both the Wu laptop and the Acronis copy as acquired *when the FBI took custody of the original laptop and Acronis copy*, not an image of what Wu had when he landed in Portland. The government is not accountable for the actions of third parties as they trample through evidence. It is, however, a matter for the jury to decide what effect, if any, to give to that conduct.

///

///

///

///

///

///

CONCLUSION

Exclusion of evidence is an extraordinary remedy limited to instances where a defendant has proven bad faith on the part of law enforcement agents who obtained the evidence and is usually reserved for constitutional violations. The matters that the defendants raise in regard to the digital evidence are relevant to the weight of that evidence, not its admissibility. Defendants' motion should be denied.

DATED this 20th day of January 2011.

Respectfully submitted,

DWIGHT C. HOLTON
United States Attorney
District of Oregon
s/ Gregory R. Nyhus
GREGORY R. NYHUS, OSB #913841
Assistant United States Attorney